# National Infrastructure Protection Center CyberNotes

*Issue #2003-03* *February 10, 2003*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between January 9 and February 6, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| 3ware Software[1] | Multiple | Disk Management Software 1.10 .020, 1.10 .012 | A Denial of Service vulnerability exists when a malicious user submits a malformed HTTP request to port 1080. | No workaround or patch available at time of publishing. | Disk Management Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[1] Bugtraq, January 30, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Allegro Software Development Corporation[2] | Multiple | RomPager version 2.00, 2.10 | A Cross-Site Scripting vulnerability exists in the embedded web server code due to inadequate filtering of user-supplied input when certain messages are displayed, which could let a remote malicious user execute arbitrary HTML and script code. | No workaround or patch available at time of publishing. | RomPager Cross Site Scripting | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Apache Software Foundation[3] | Unix | Tomcat 3.0- 3.3.1 | Multiple vulnerabilities exist: a directory/file disclosure vulnerability exists due to improper handling of null bytes and backslash characters in requests for web resources, which could let a remote malicious user obtain sensitive information; a file disclosure vulnerability exists because it is possible to create a malicious 'web.xml' file, which could let a malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in sample web applications, which could let a remote malicious user execute arbitrary code. | This issue will reportedly be addressed by the vendor in Tomcat 3.3.2.<br>**Debian:**<br>http://security.debian.org/pool/updates/contrib/t/tomcat/<br>**Apache** (corrects the directory/file disclosure vulnerabilities)**:**<br>http://jakarta.apache.org/builds/jakarta-tomcat/release/v3.3.1a/ | Tomcat Multiple Vulnerabilities<br>CVE Names: CAN-2003-0042, CAN-2003-0043, CAN-2003-0044 | Medium/ **High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |
| Astaro[4] | Unix | Security Linux Firewall 3.214 & prior | An access control vulnerability exists, which could let a remote malicious traverse the firewall. | Patch available at:<br>http://www.astaro.org/ubb/ultimatebb.php?ubb=get_topic;f=1;t=000144 | Astaro Security Linux Firewall HTTP Proxy | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[2] Securiteam, January 18, 2003.
[3] Debian Security Advisory, DSA 246-1, January 29, 2003.
[4] Bugtraq, January 20, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| BEA Systems, Inc.[5] | Windows NT 4.0/2000, XP, Unix | WebLogic Express 5.1 5.1 SP1-SP13, WebLogic Express 6.0, 6.0 SP1&SP2, 6.1, 6.1 SP1-SP4, 7.0, 7.0 SP1, 7.0.0.1, 7.0.01 SP1, WebLogic Express for Win32 5.1, SP1- SP13, 6.0, 6.0 SP1, 6.1, 6.1 SP1-SP4, 7.0, 7.0 SP1, 7.0.0.1, 7.0.0.1 SP1, WebLogic Server 5.1, 5.1 SP1-SP13, 6.0, 6.0 SP1&SP2, 6.1 SP1-SP4, 7.0, 7.0 SP1, 7.0.0.1, 7.0.0.1 SP1, WebLogic Server for Win32 5.1, 5.1 SP1-SP13, 6.0, 6.0 SP1, 6.1, 6.1 SP1-SP4, 7.0, 7.0 SP1, 7.0.0.1, 7.0.0.1 SP1 | Multiple vulnerabilities exist: a vulnerability exists due to a race condition when the software is used in a clustered environment, which could let a malicious user obtain sensitive information; and a vulnerability exists because passwords can be recovered when keystores are used, which could let a malicious user obtain unauthorized access. | Patches available at:<br>ftp://ftpna.beasys.com/pub/releases/security | WebLogic Server and Express Multiple Vulnerabilities | Medium | Bug discussed in newsgroups and websites. |

[5] Security Advisory, BEA03-26.00, January 29, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Blackboard[6] | Multiple | Blackboard 5.0, 5.0.2, 5.5, 5.5.1 | A vulnerability exists in the 'search.pl' script file due to insufficient sanitization of user-supplied SQL query input, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Blackboard search.pl SQL Sensitive Information | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Bladeenc[7] | Windows, Unix | Bladeenc 0.92.7, 0.93.10, 0.94.0 - 0.94.2 | A vulnerability exists in the MP3 media encoder, which could let a malicious user execute arbitrary code. | It has been reported that this product is no longer being maintained by the vendor. | Bladeenc Signed Integer Memory Corruption | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published. |
| **Brown Bear Software[8]**<br>***Upgrade now available[9]*** | **Windows 95/98/NT 4.0/2000, XP** | **iCal 3.7** | **Two vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious user submits a specially formatted HTTP request; and a buffer overflow vulnerability exists when an overly long HTTP request is submitted, which could let a malicious user cause a Denial of Service.** | ***Upgrade available at:*** **http://www.brownbearsoftware.com/ical/icalv38.exe** ***Vendor upgrade instructions:*** **http://www.brownbearsw.com/ical/icalupgrade.html** | **iCal Remote Denial of Service Vulnerabilities** | **Low** | **Bug discussed in newsgroups and websites.** |
| Byte/400[10] | Windows | Platinum FTPserver 1.0.6, 1.0.7 | Multiple vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and a Denial of Service vulnerability exists due to a failure to properly sanitize FTP commands. | Upgrade available at: http://www.platinumftp.com/Updates/PlatinumFTPserver.exe | PlatinumFTP Server Multiple Vulnerabilities | Low/ Medium<br>(Medium if sensitive information is obtained) | Bug discussed in newsgroups and websites. Exploit has been published. |
| Celestial Software[11] | Windows 95/98/NT 4.0/2000 | Absolute Telnet 2.11 | A vulnerability exists because password authentication information is handled in an unsafe manner, which could let a malicious user obtain sensitive information. | A beta version available at: http://www.celestialsoftware.net/telnet/beta_software.html | AbsoluteTelnet Authentication Password<br>CVE Name: CAN-2003-0046 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |

[6] Bugtraq, January 24, 2003.
[7] Bugtraq, February 2, 2003.
[8] Bugtraq, January 3, 2003.
[9] SecurityFocus, January 28, 2003.
[10] Securiteam, January 13, 2003.
[11] iDEFENSE Security Advisory, January 28, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Cisco Systems[12] | Multiple | Cisco Building Broadband Service Manager 5.0, 5.1, Call Manager 3.3, Unity Server 3.0-3.3, 4.0 | A number of vulnerabilities that have been discovered that enable a malicious user to execute arbitrary code or cause a Denial of Service against the server. These vulnerabilities were discovered and publicly announced by Microsoft in their Microsoft Security Bulletins MS02-039, MS02-056, and MS02-061. All Cisco products and applications that are using unpatched Microsoft SQL Server 2000 or MSDE 2000 are vulnerable. | Patch information available at:<br>http://www.cisco.com/warp/public/707/cisco-sa-20030126-ms02-061.shtml | SQL Server Web Task Stored Procedure Privilege Escalation<br>**CVE Name: CAN-2002-1145** | Low/**High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. Vulnerability exploited by the Slammer worm.<br>Vulnerability has appeared in the press and other public media. |
| Citrix[13] | Windows 2000 | MetaFrame XPe | A vulnerability exists when the server is configured on Novell Networks because in some cases a remote authenticated user may obtain the access privileges of another authenticated user on the same server, which could let a remote malicious user obtain elevated privileges. | No workaround or patch available at time of publishing. | MetaFrame Server Remote Elevated Privileges | Medium | Bug discussed in newsgroups and websites. |
| Compaq[14] | Windows | Insight Manager 7.0, 7.0 SP1 | A vulnerability exists if an authenticated user doesn't manually logout from the Web Agents interface because sessions continue until expiration after an authenticated user closes their browser, which could let a malicious user obtain unauthorized access or perform actions with elevated privileges. | No workaround or patch available at time of publishing. | HP Compaq Insight Manager/ Compaq Web Agent Session Persistence | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |

[12] Cisco Security Advisory, January 27, 2003.
[13] Bugtraq, January 21, 2003.
[14] Bugtraq, January 30, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **CVS**[15, 16, 17, 18, 19, 20]<br>***More vendors release patches***[21, 22] | **Unix** | **CVS 1.10.7, 1.10.8, 1.11 1.11.1 p1, 1.11.1-1.11.4** | **A double free vulnerability exists in Directory requests, which could let an unauthorized remote malicious user execute arbitrary code.** | **IBM:**<br>**ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/RPMS/ppc/cvs/cvs-1.11.1p1-3.aix4.3.ppc.rpm**<br>**Debian:**<br>**http://security.debian.org/pool/updates/main/c/cvs/**<br>**Mandrake:**<br>**http://www.mandrakesecure.net/en/ftp.php**<br>**Conectiva:**<br>**ftp://atualizacoes.conectiva.com.br/**<br>**CVS:**<br>**http://ccvs.cvshome.org/servlets/ProjectDownloadList**<br>**RedHat:**<br>**ftp://updates.redhat.com/**<br>**OpenBSD:**<br>**ftp://ftp.openbsd.org/pub/OpenBSD/patches/**<br>**Slackware:**<br>**ftp://ftp.slackware.com/pub/slackware/**<br>***FreeBSD:***<br>**ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:01/cvs.patch**<br>***SCO:***<br>**ftp://ftp.sco.com/pub/updates/OpenLinux/** | **CVS Directory Request Double Free Code Execution**<br>**CVE Name: CAN-2003-0015** | **High** | **Bug discussed in newsgroups and websites.**<br>***Exploit has been published.*** |
| dotmar-keting, Inc. [23] | Windows, Unix | dotproject dev 20030121 | A vulnerability exists in the 'core.php' script due to inadequate security checking, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | 'dotproject' 'core.php' Script | High | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Double Precision Incorpor-ated[24] | Unix | Courier MTA 0.37.3; Inter7 Courier-IMAP 1.6 | A vulnerability exists in Courier-IMAP when running in conjunction with a PostgreSQL database due to insufficient sanitization of usernames during authentication, which could let a malicious user execute arbitrary SQL commands. | Upgrade available at:<br>http://www.inter7.com/courierframe.html<br>**Debian:**<br>http://security.debian.org/pool/updates/main/c/courier-ssl/ | Courier-IMAP Username SQL Injection<br>CVE Name: CAN-2003-0040 | High | Bug discussed in newsgroups and websites. |

[15] Conectiva Linux Security Announcement, 2003-01-23, January 23, 2003.
[16] Gentoo Linux Security Announcement, 0301-12, January 23, 2003.
[17] CERT Advisory, CA-2003-02, January 23, 2003.
[18] Debian Security Advisory, DSA 233-1, January 21, 2003.
[19] Mandrake Linux Security Update Advisory, MDKSA-2003:009, January 20, 2003.
[20] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:012-07, January 20, 2003.
[21] FreeBSD Security Advisory, FreeBSD-SA-03:01, February 4, 2003.
[22] SCO Security Advisory, CSSA-2003-006.0, January 31, 2003.
[23] Securiteam, January 30, 2003.
[24] Debian Security Advisory, DSA 247-1, January 30, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Electra Soft[25] | Windows NT | 32Bit FTP 9.49.1 | A buffer overflow vulnerability exists when a banner that contains an excessive amount of data is submitted, which could let a remote malicious user execute arbitrary code. | Upgrade available at:<br>http://www.electrasoft.com/32ftp.htm | 32Bit FTP Long Server Banner Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Emilio Jose Jimenez[26] | Windows, Unix | TOPo 1.43 | A vulnerability exists when an invalid parameter is specified in the 'in.php' or 'out.php' scripts, which could let a remote malicious user obtain sensitive information. | Upgrade available at:<br>http://ej3scripts.loadedweb.com/modules.php?name=Info_Scripts&file=index&func=topo | TOPo Remote Path Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Epic Games[27] | Multiple | Unreal Engine 436, 433, 226f | Multiple vulnerabilities exist: a vulnerability exists due to the way specially crafted packets are handled, which could let a malicious user cause a Denial of Service: a vulnerability exits when numerous packets that request to join are submitted to the game server, which could let a malicious user cause a Denial of Service; a vulnerability exists when a file is created that contains a large negative index value, which could let a malicious user execute arbitrary code; a vulnerability exists because it is possible to use a game server as an amplifier in a flooding attack; a vulnerability exists when multiple UDP packets are transmitted that contain a spoofed victim IP address, which could let a malicious user cause a Denial of Service; a vulnerability exists when the game client connects to a server using a excessive length Unreal URL, which could let a malicious user cause a Denial of Service; a Directory Traversal vulnerability exists which could let a malicious user obtain sensitive information; and a vulnerability exists when a malicious user refers to specific files which could cause a Denial of Service. | No workaround or patch available at time of publishing. | Unreal Engine Multiple Vulnerabilities | Low/ Medium/ **High**<br>**(Low if a Denial of Service, Medium is sensitive information can be obtained, and High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |

[25] SecurityFocus, February 4, 2003.
[26] Bugtraq, February 4, 2003.
[27] SecurityFocus, February 5, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Eric Raymond**[28, 29, 30, 31, 32, 33, 34]<br><br>**More patches released**[35, 36, 37] | **Unix** | **Fetchmail 5.3.3, 5.4-5.6, 5.6.5, 5.7-5.9.14, 6.0.0, 6.1.0, 6.1.3** | **A buffer overflow vulnerability exists when a reply-hack action is performed, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.** | **Debian:**<br>**http://security.debian.org/pool/updates/main/f/fetchmail/**<br>**Fetchmail:**<br>**http://www.tuxedo.org/~esr/fetchmail/fetchmail-6.2.0.tar.gz**<br>**SuSE:**<br>**ftp://ftp.suse.com/pub/suse/**<br>**RedHat:**<br>**ftp://updates.redhat.com/**<br>**Conectiva:**<br>**ftp://atualizacoes.conectiva.com.br**<br><br>***SCO:***<br>**ftp://ftp.sco.com/pub/updates/**<br>***EnGarde:***<br>**http://ftp.engardelinux.org/pub/engarde/stable/updates**<br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/ftp.php** | **Fetchmail Buffer Overflow**<br><br>**CVE Name: CAN-2002-1365** | **Low/High**<br><br>**(High if arbitrary code can be executed)** | **Bug discussed in newsgroups and websites.** |

[28] e-matters GmbH Security Advisory, 05/2002, December 13, 2002.
[29] Gentoo Linux Security Announcement, 200212-3, December 15, 2002.
[30] Conectiva Linux Security Announcement, CLA-2002:554, December 16, 2002.
[31] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:293-09, December 17, 2002.
[32] OpenPKG Security Advisory, OpenPKG-SA-2002.016, December 17, 2002.
[33] Debian Security Advisory, DSA 216-1, December 24, 2002.
[34] SuSE Security Announcement, SuSE-SA:2003:001, January 2, 2003.
[35] SCO Security Advisory, CSSA-2003-001.0, January 9, 2003.
[36] EnGarde Secure Linux Security Advisory, ESA-20030127-002, January 27, 2003.
[37] Mandrake Linux Security Update Advisory, MDKSA-2003:011, January 27, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Finjan Software[38] | Windows NT, Unix | SurfinGate 5.6 | Multiple vulnerabilities exist: a vulnerability exists in Console and Oracle passwords due to weak encryption algorithms, which could let a malicious user obtain sensitive information; a vulnerability exists because the HTML filter inadequately recognizes certain types of malicious HTML, which could let a malicious user cause a Denial of Service; a vulnerability exists in the JavaScript parser due to insufficient sanitization of user-supplied code, which could let a malicious user execute arbitrary JavaScript code; a vulnerability exists because the Java applet analyzer does not properly detect the use of the Java Reflection API, which could let a malicious user bypass the filters and execute arbitrary malicious Java applets; a vulnerability exists because file filtering rules can be circumvented, which could let a malicious user bypass security restrictions; and a vulnerability exists due to inadequate dissection of archive files, which could let a malicious user bypass security restrictions and execute arbitrary code. | For workarounds and upgrades see:<br>http://www.csnc.ch/downloads/docs/techdocs/FinjanSurfinGate_Analysis_CSNC_V3.0.pdf<br>Some of these vulnerabilities don't exist in the current version, SurfinGate 7.0. | SurfinGate Multiple Vulnerabilities | Medium/ **High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. |
| Francisco Burzi[39] | Windows, Unix | PHP-Nuke 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0 | An input validation vulnerability exists in the avatar feature due insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | PHP-Nuke Avatar Input Validation | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| FTLS.org[40] | Unix | Guestbook 1.1 | A vulnerability exists due to inadequate filtering of HTML tags, which could let a malicious user execute arbitrary script code. | No workaround or patch available at time of publishing. | GuestBook Script Injection | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[38] Compass Security Team Advisory, January 27, 2003.
[39] Bugtraq, February 2, 2003.
[40] Bugtraq, January 25, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Gilbert Murgallis[41] | Unix | List Site Pro 2.0 | A vulnerability exists because a remote user can submit specially crafted data when signing up for a user account to gain access to a target user's account, which could let a remote malicious user obtain unauthorized access. | No workaround or patch available at time of publishing. | List Site Pro Account Hijack | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| GNU[42] | Unix | Mailman 2.1 | A Cross-Site Scripting vulnerability exists in the mailing list distribution software and default error page due to insufficient sanitization of URI parameters, which could let a remote malicious user execute arbitrary HTML and script code. | Patch available at: http://twtelecom.dl.sourceforge.net/sourceforge/mailman/xss-2.1.0-patch.txt | Mailman Remote Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Great Circle Associates[43] | Unix | Majordomo 1.94.4, 1.94.5, 2.0 | A vulnerability exists in the default configuration because list subscriber information is inadequately protected, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Majordomo Remote List Subscriber Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Greg Billock[44] | Windows, Unix | EditTag 1.1 | A vulnerability exists in the 'edittag.pl' Perl script due to insufficient sanitization of CGI parameters, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | EditTag edittag.pl Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Hypermail[45] | Unix | Hypermail 2.1.3, 2.1.4, 2.1.5 | Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the parsemail() function, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'mail' CGI component when a reverse DNS lookup is performed if the hostname is of excessive length, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the mail CGI program, which could let a remote malicious user send e-mail to arbitrary recipients. | Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=18117&release_id=135937 | Hypermail Remote Buffer Overflows | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |

[41] Bugtraq, January 25, 2003.
[42] SecurityFocus, January 27, 2003.
[43] Bugtraq, February 4, 2003.
[44] Bugtraq, January 24, 2003.
[45] Bugtraq, January 27, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| IBM[46] | Windows NT 4.0, Unix | WebSphere Application Server 2.0, 3.0.2-3.0.2.4, 3.0, 3.5-3.5.3, 4.0.3, WebSphere Application Server Advanced Edition 3.0.2.1, 4.0.4, 4.0 | A vulnerability exists because passwords in WebSphere XML configuration export are not sufficiently protected, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | WebSphere Exported XML Password Encoding | Medium | Bug discussed in newsgroups and websites. |
| **ISC**[47]<br>***Debian releases patch***[48] | **Unix** | **DHCPD 3.0.1 1 rc1-rc10** | **A remote Denial of Service vulnerability exists in 'dhcrelay' when a malicious bootp packet is submitted.** | **Debian:**<br>**http://security.debian.org/pool/updates/main/d/dhcp3/** | **DHCPD dhcrelay Extraneous Network Packets Remote Denial of Service**<br>**CVE Name: CAN-2003-0039** | **Low** | **Bug discussed in newsgroups and websites. Exploit has been published.** |
| Jan Kneschke[49] | Unix | ModLogAn 0.8.3 & prior | A vulnerability exists in the exists in the url_decode() function, which could let a remote malicious user execute arbitrary code. | Upgrade available at:<br>http://jan.kneschke.de/projects/modlogan/download/ | ModLogAn URL Decoding | **High** | Bug discussed in newsgroups and websites. |
| Julien Desaunay[50] | Windows, Unix | phpMy Shop 1.0 | A vulnerability exists in the 'compte.php' script file due to insufficient sanitization of user-supplied input when constructing SQL queries, which could let a remote malicious execute arbitrary code. | No workaround or patch available at time of publishing. | phpMyShop compte.php SQL Injection | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| **KDE**[51, 52]<br>***More patches released***[53, 54] | **Unix** | **KDE 2.0, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5** | **Multiple vulnerabilities exist due to a failure to properly quote parameters of instructions passed to a command shell for execution, which could let a local/remote malicious user execute arbitrary commands.** | **Upgrade available at:**<br>**http://download.kde.org/stable/3.0.5a/**<br>**Debian:**<br>**http://security.debian.org/pool/updates/main/k/kdeadmin/** | **KDE Parameter Quoting Shell Command Execution**<br>**CVE Name: CAN-2002-1393** | **High** | **Bug discussed in newsgroups and websites.** |

[46] Compass Security Advisory, February 4, 2003.
[47] Bugtraq, January 15, 2003.
[48] Debian Security Advisory, DSA 245-1, January 28, 2003.
[49] SecurityFocus, January 23, 2003.
[50] Bugtraq, February 3, 2003.
[51] KDE Security Advisory, December 21, 2002.
[52] Gentoo Linux Security Announcement, 200212-9, December 22, 2002.
[53] Gentoo Linux Security Announcement ,200301-11, January 18, 2003.
[54] Debian Security Advisories, DSA 234-1- 238-1, January 22 & 23, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Macromedia[55] | Windows NT 4.0/2000, XP | ColdFusion Server MX Professional, Enterprise, Developer, 6.0 | A vulnerability exists because user permissions are not properly validated when used in conjunction with Microsoft IIS, Windows NT authentication, and NTFS file permissions, which could let a remote malicious user obtain unauthorized access to ColdFusion templates and directories. | Workaround available at:<br>http://www.macromedia.com/v1/handlers/index.cfm?ID=23734 | ColdFusion MX Windows User File Authorization | Medium | Bug discussed in newsgroups and websites. |
| Macromedia[56] | Multiple | Shockwave 1.0, 2.0, 3.0, 4.0, 5.0 | A vulnerability exists in the multimedia playback application, which could let a malicious user create a Shockwave movie that will disclose sensitive information. | Macromedia reports that this issue has been resolved in Shockwave version 6. Users of products prior to this are advised to update to the current versions. | Shockwave File Disclosure<br>CVE Name: CAN-1999-1525 | Medium | Bug discussed in newsgroups and websites. |
| Martin Prikryl[57] | Multiple | WinSCP 2.2 | A vulnerability exists because password authentication information is handled in an unsafe manner, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | WinSCP SSH2 Authentication Password | Medium | Bug discussed in newsgroups and websites. |
| **Mcrypt**[58, 59]<br>***More vendors release advisories*** [60, 61]<br>***More Vendors release advisories*** [62, 63] | **Unix** | **libmcrypt 2.5.1 -r4, 2.5.2, 2.5.3** | **Multiple buffer overflow vulnerabilities exist in various functions that are used to process user-supplied input due to insufficient bounds checking, which could let a malicious user execute arbitrary code.** | **Upgrade available at: http://mcrypt.hellug.gr/lib/index.html**<br>***Debian:*** http://security.debian.org/pool/updates/main/libm/libmcrypt/<br>***SuSE:*** ftp://ftp.suse.com/pub/suse<br>***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/**<br>***Debian:*** **http://security.debian.org/pool/updates/main/libm/libmcrypt/** | **Libmcrypt Multiple Buffer Overflow Vulnerabilities**<br>**CVE Names: CAN-2003-0031, CAN-2003-0032** | **High** | **Bug discussed in newsgroups and websites.** |

[55] Macromedia Security Bulletin, MPSB03-02, January 30, 2003.
[56] SecurityFocus, January 24, 2003.
[57] SecurityFocus, January 30, 2003.
[58] Bugtraq, January 3, 2003.
[59] Gentoo Linux Security Announcement, 200301-4, January 5, 2003.
[60] Debian Security Advisory, DSA 228-1, January 14, 2003.
[61] SuSE Security Announcement, SuSE-SA:2003:0004, January 14, 2003.
[62] Conectiva Linux Security Announcement, CLA-2003:567, February 5, 2003.
[63] Debian Security Advisory, DSA 228-1, January 14, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[64]<br>*Microsoft re-releases bulletin*[65, 66] | Windows NT 4.0/2000 | Data Engine 1.0, 2000, SQL Server 7.0, SQL Server 7.0 SP1-SP4, SQL Server 2000, SQL Server 2000 SP1&2 | A vulnerability exists because there is a flaw in the stored procedure that runs web tasks due to the way permissions are handled, which could let a malicious user obtain elevated privileges. In addition, there are weak permissions on the web tasks table that together with the stored procedure could allow a malicious user to run, delete or update a web task.<br>*Note: This patch supersedes the one provided in Microsoft Security Bulletin MS02-056, which was also a cumulative patch.*<br>*Microsoft has re-released the patch for SQL Server 2000. It has been re-released to help customers patch their systems in response to the "Slammer" worm  virus. The re-released patch integrates the original security patch released with this bulletin and the hotfix discussed in Microsoft Knowledge Base article 317748 that was released to ensure the correct operation of SQL Server. The re-release has been packaged with a new SQL Server patch installer. The installer eliminates the need for system administrators to copy SQL Server files onto their systems manually. The only changes that Microsoft has made to this patch were to incorporate the hotfix discussed in Microsoft Knowledge Base article 317748 into the re-released patch and to package the patch with an installer.* | Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp<br>*Note: This is a cumulative patch that includes the functionality of all previously released patches for SQL Server 7.0, SQL Server 2000, and Microsoft Data Engine (MSDE) 1.0, Microsoft Desktop Engine (MSDE) 2000. In addition, it eliminates one newly discovered vulnerability.* | Microsoft SQL Server Web Task Stored Procedure Privilege Escalation<br>CVE Name: CAN-2002-1145 | Very High due to the SQL worm | Bug discussed in newsgroups and websites.<br>*Vulnerability exploited by the SQL worm.* |

[64] Microsoft Security Bulletin, MS02-061, October 16, 2002.
[65] Microsoft Security Bulletin MS02-061 V2.2, January 27, 2003.
[66] Microsoft Security Bulletin MS02-061 V2.3, January 28, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[67] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 5.0.1, 5.0.1 SP1-SP3, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1 | Several vulnerabilities exist: a vulnerability exists because it is possible to bypass the cross-domain security model that Internet Explorer uses when using dialog boxes, which could let a malicious user execute arbitrary code; and a vulnerability exists because it is possible to bypass the cross-domain security model that Internet Explorer implements when using showHelp () functionality, which could let a malicious user execute arbitrary commands. | Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-004.asp<br>*Note: Reports indicate that this patch may not install correctly through the WindowsUpdate website. Users are encouraged to download and install the patch manually.* | Internet Explorer Cross-Domain Vulnerabilities<br>CVE Names: CAN-2003-1326, CAN-2003-1328 | High | Bug discussed in newsgroups and websites. |
| Microsoft[68] | Windows 95/98/ME/ NT 4.0/2000 | Internet Explorer 5.5, 5.5 SP1&SP2, 6.0, 6.0 SP1 | A vulnerability exists when the dragDrop() ActiveX method is used, which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Internet Explorer dragDrop Method | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published. |
| **Microsoft**[69]<br>***Microsoft re-releases bulletin***[70] | **Windows NT 4.0/2000** | **Data Engine 1.0, 2000, SQL Server 7.0. SQL Server 7.0 SP1-4, SQL Server 2000, SQL Server 2000 SP1&2,** | **A vulnerability exists in some of the extended stored procedures due to weak permissions, which could let a malicious user obtain unauthorized administrator privileges.**<br>***The patch released with this bulletin is effective in protecting SQL Server 2000 and MSDE 2000 against the "SQL Slammer" worm virus. However, this patch has been superseded by the patch released with MS02-061, which contains fixes for additional security vulnerabilities in these products.*** | **Frequently asked questions regarding this vulnerability and the patch can be found at:**<br>**http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-043.asp**<br>***Microsoft recommends that SQL 2000 and MSDE 2000 customers apply the patch from MS02-061 available at:***<br>**http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-061.asp** | **Microsoft SQL Server Extended Stored Procedure Privilege Elevation**<br>**CVE Name: CAN-2002-0721** | **High** | **Bug discussed in newsgroups and websites.**<br>***Exploit script has been published.***<br>***Vulnerability is exploited by the SQL worm that has been reported in the wild.***<br>***Vulnerability has appeared in the press and other public media.*** |

[67] Microsoft Security Bulletin, MS03-004 V1.1, February 6, 2003.
[68] Bugtraq, February 3, 2003.
[69] Microsoft Security Bulletin, MS02-043, August 14, 2002.
[70] Microsoft Security Bulletin, MS02-043 V1.1, January 31, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Microsoft** [71]<br>***Microsoft re-releases bulletin*** [72] | **Windows NT 4.0/2000** | **Data Engine 1.0, 2000; SQL Server 7.0, 7.0 SP1-SP4, 2000, 2000 SP1&2** | **Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the section of code in SQL Server 2000 (and MSDE 2000) associated with user authentication, which could let a malicious user cause a Denial of Service or execute arbitrary code with the privileges of the SQL Server process; a buffer overflow vulnerability exists in the one of the Database Console Commands (DBCCs) that ship as part of SQL Server 7.0 and 2000, which could let a malicious user execute arbitrary code with the privileges of the SQL Server process; and a vulnerability exists due to the way scheduled jobs in SQL Server 7.0 and 2000 are handled, which could let a malicious user execute arbitrary operating system commands with elevated privileges.**<br>***The patch released with this bulletin is effective in protecting SQL Server 2000 and MSDE 2000 against the "SQL Slammer" worm virus. However, this patch has been superseded by the patch released with MS02-061, which contains fixes for additional security vulnerabilities in these products.*** | **Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/ technet/treeview/default.asp?url=/technet/security/bulletin/MS02-056.asp**<br>***Microsoft recommends that SQL 2000 and MSDE 2000 customers apply the patch from MS02-061 available at:*** **http://microsoft.com/technet/treeview/default.asp?url =/technet/security/bulletin/ ms02-061.asp** | **Multiple Microsoft SQL Server Vulnera-bilities**<br>**CVE Names: CAN-2002-1123, CAN-2002-1137, CAN-2002-1138** | **Low/High**<br>**(High if arbitrary code can be executed)** | **Bug discussed in newsgroups and websites.**<br>**Vulnerability has appeared in the press and other public media.**<br>***Exploit script has been published.***<br>***Vulnerability is exploited by the SQL worm that has been reported in the wild.*** |
| Microsoft [73] | Windows 2000, XP | Windows 2000 Server, SP1-SP3, 2000 Terminal Services SP1-SP3, XP Profes-sional, SP1 | A remote Denial of Service vulnerability exists in the Microsoft Graphical Identification and Authentication DLL (MSGINA.DLL). | No workaround or patch available at time of publishing. | Windows MSGINA.DLL Remote Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[71] Microsoft Security Bulletin, MS02-056, October 2, 2002.
[72] Microsoft Security Bulletin, MS02-056 V1.2, January 31, 2003.
[73] Bugtraq, January 23, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft[74] | Windows XP | Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1 | A vulnerability exists in the implementation of the Windows Redirector because an unchecked buffer is used to receive parameter information, which could let a malicious user cause a Denial of Service or execute arbitrary code. | Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-005.asp | Windows XP Redirector Buffer Overflow<br>CVE Name: CAN-2003-0004 | Low/**High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. |
| Microsoft[75] | Windows 2000 | Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3 | A vulnerability exists when NetBIOS continuation packets are handled, which could let a malicious user cause a Denial of Service. | No workaround or patch available at time of publishing. | Windows 2000 NetBIOS Continuation Packets Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Microsoft[76] | Windows 2000 | Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3 | A vulnerability exists when a Denial of Service is caused against the RPC service, which could let a remote malicious obtain elevated privileges. | No workaround or patch available at time of publishing. | Windows 2000 RPC Service Privilege Escalation | Medium | Bug discussed in newsgroups and websites. |

[74] Microsoft Security Bulletin, MS03-005, February 5, 2003.
[75] Bugtraq, February 4, 2003.
[76] SecurityFocus, February 4, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Microsoft [77]<br>*SQL worm reported in the wild[78]* | Windows NT 4.0/2000 | SQL Server 2000, 2002 SP1&2 | Three vulnerabilities exist: two buffer overflow vulnerabilities exist in the resolution service when a maliciously crafted UDP packet is sent, which could let a remote malicious user execute arbitrary code; and a Denial of Service vulnerability exists when a malicious user sends a particular data packet to the SQL server's keep-alive function.<br>*W32.Slammer is a memory resident worm that propagates via UDP Port 1434 and exploits a vulnerability in SQL Server 2000 systems and systems with MSDE 2000 that have not applied the patch released by Microsoft Bulletin MS02-039.* | Frequently asked questions regarding this vulnerability and the patch can be found at:<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp<br>*Depending on which product customers are using there may be different methods Microsoft recommends to secure your product. Information is available at:*<br>http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/slammer.asp | Microsoft SQL Server 2000 Multiple Vulnerabilities<br>CVE Names: CAN-2002-0649, CAN-2002-0650 | Low/High<br>(High if arbitrary code can be executed) | Bug discussed in newsgroups and websites.<br>Vulnerability has appeared in the press and other public media.<br>*Exploit script has been published.*<br>*Vulnerability is exploited by the SQL worm, which has been reported in the wild.*<br>*Vulnerability has appeared in the press and other public media.* |

[77] Microsoft Security Bulletin, MS02-039, July 24, 2002.

[78] PSS Security Response Team Alert, January 30, 20003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Microsoft**[79]<br>***Microsoft re-releases bulletin***[80] | **Windows NT 4.0/2000, XP** | **Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, XP Home, XP Home SP1, XP Professional, XP Professional SP1** | **A vulnerability exists because it's possible for one process in the interactive desktop to use a WM_TIMER message to cause another process to execute a callback function at the address of its choice, even if the second process did not set a timer, which could let a malicious user obtain full administrative privileges.**<br>***After the bulletin was released, it was determined that the patch for Windows NT 4.0 machines introduced an error that may, under certain configurations, cause NT 4.0 to fail. Microsoft is investigating this issue and will shortly release an updated patch for Windows NT 4.0. The bulletin has been updated to remove the download links for the NT 4.0 patch and will be revised again once the updated package is available. Customers who have installed the patch on Windows 2000 and Windows XP are unaffected by this error.*** | **Frequently asked questions regarding this vulnerability and the patch can be found at:**<br>**http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-071.asp** | **Windows 2000/XP WM_TIMER Message Handling**<br>**CVE Name: CAN-2002-1230** | **High** | **Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.**<br>***Vulnerability has appeared in the press and other public media.*** |
| MIT[81] | Unix | Kerberos 5 1.2.1-1.2.4 | Multiple vulnerabilities exist: a vulnerability exists in various 'printf' functions due to a failure to supply sufficient format specifiers when handling user-supplied data, which could let a malicious user execute arbitrary commands; and a vulnerability exists due to insufficient bounds checking and sanitization of user-supplied data, which could let a remote malicious user cause a Denial of Service. | Upgrade available at:<br>http://web.mit.edu/kerberos/www/krb5-1.2/index.html | Kerberos Key Distribution Center Vulnerabilities | Low/<br>**High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. |

[79] Microsoft Security Bulletin, MS02-071, December 11, 2002.
[80] Microsoft Security Bulletin, MS02-071 V1.2, February 03, 2003.
[81] MIT krb5 Security Advisory, MITKRB5-SA-2003-001, January 28, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| MIT[82] | Unix | Kerberos 5 1.2.1, 1.2.2 | A vulnerability exists due to insufficient realm transit path verification, which could let a malicious user forge the identity of other users. | Upgrade available at:<br>http://web.mit.edu/kerberos/www/krb5-1.2/index.html | Kerberos / Key Distribution Center Shared Key User Spoofing | Medium | Bug discussed in newsgroups and websites. |
| Mollensoft Software[83] | Windows NT 4.0/2000 | Enceladus Server Suite 3.9 | A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Enceladus Server Suite Information Disclosure | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| **Multiple Vendors[84]**<br>***RedHat releases patches[85]*** | **Windows 2000, Unix** | **FreeBSD 4.2-4.7; Linux kernel 2.4.1-2.4.20; Microsoft Windows 2000 Advanced Server, SP1-SP2, 2000 Datacenter Server, SP1-SP2, 2000 Professional, SP1-SP2, 2000 Server, SP1-SP2, 2000 Terminal Services, SP1-SP2; NetBSD NetBSD 1.5- 1.5.3, 1.6** | **A vulnerability exists because multiple platform Ethernet Network Interface Card (NIC) device drivers incorrectly handle frame padding due to incorrect implementations of RFC requirements and poor programming practices, which could let a malicious user obtain sensitive information.** | **No workaround or patch available at time of publishing.**<br>***RedHat:***<br>**ftp://updates.redhat.com/** | **Multiple Vendor Network Device Driver Frame Padding Information Disclosure**<br>**CVE Name: CAN-2003-0001** | **Medium** | **Bug discussed in newsgroups and websites.**<br>**Vulnerability has appeared in the press and other public media.** |
| Multiple Vendors[86, 87] | Unix | Linux kernel 2.4.10-2.4.19 | A vulnerability exists because the O_DIRECT flag is not handled properly, which could let a malicious user obtain sensitive information. | **RedHat:**<br>ftp://updates.redhat.com/<br>**Mandrake:**<br>http://www.mandrakesecure.net/en/ftp.php | Linux O_DIRECT Information Leak | Medium | Bug discussed in newsgroups and websites. |

[82] MIT krb5 Security Advisory, MITKRB5-SA-2003-001, January 28, 2003.
[83] VulnWatch, January 21, 2003.
[84] @stake, Inc. Security Advisory, A010603-1, January 7, 2003.
[85] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:025-20, February 4, 2003.
[86] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:025-20, February 4, 2003.
[87] Mandrake Linux Security Update Advisory, MDKSA-2003:014, February 5, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Multiple Vendors**[88]<br>***More Vendors release advisories*** [89, 90] | **Unix** | **Linux kernel 2.4.1-2.4.18** | **A Denial of Service vulnerability exists when a malicious user triggers a system call with the TF flag enabled.** | **Upgrade available at:**<br>**ftp://ftp.kernel.org/pub/linux/kernel/v2.4/linux-2.4.19.tar.bz2**<br>***Conectiva:***<br>**ftp://atualizacoes.conectiva.com.br/7.0/RPMS**<br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/ftp.php** | **Linux Kernel 2.4 System Call TF Flag Denial of Service** | **Low** | **Bug discussed in newsgroups and websites. Exploit has been published.** |
| MySQL AB[91, 92] | Unix | MySQL 3.23.52-3.23.54 | A Denial of Service vulnerability exists due to a double free() pointer bug in the way mysql_change_user() is handled. | **MySQL:**<br>http://www.mysql.com/downloads/mysql-3.23.html<br>**OpenPKG:**<br>ftp://ftp.openpkg.org/release<br>**Mandrake:**<br>http://www.mandrakesecure.net/en/ftp.php | MySQL Double Free Denial of Service | Low | Bug discussed in newsgroups and websites. There is no exploit code required. |

[88] Bugtraq, November 11, 2002.
[89] Conectiva Linux Security Announcement, CLA-2002:553, December 16, 2002.
[90] Mandrake Linux Security Update Advisory, MDKSA-2003:014, February 5, 2003.
[91] Mandrake Linux Security Update Advisory, MDKSA-2003:013, February 4, 2003.
[92] OpenPKG Security Advisory, OpenPKG-SA-2003.008, January 29, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **MySQL AB**[93, 94, 95, 96, 97, 98, 99, 100, 101]<br>***More advisories issued***[102, 103] | **Unix** | **MySQL 3.20.32 a, 3.22.26-3.22.30, 3.22.32, 3.23.2-3.23.5, 3.23.8-3.23.10, 3.23.23-3.23.31, 3.23.33, 3.23.34, 3.23.36-3.23.53, 4.0.0-4.0.3, 4.0.5 a** | **Several vulnerabilities exist: a vulnerability exists in the password authentication mechanism, which could let a malicious user obtain unauthorized database access; a vulnerability exists in the COM_CHANGE_USER command due to insufficient bounds checking, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the read_rows function because stored row sizes are not verified by the client, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.** ***A vulnerability also exists when COM_TABLE_ DUMP malformed commands are issued, which could let a malicious user cause a Denial of Service.***<br>***NOTE: The updates provided in the EnGarde Advisory, ESA-20021213-033 missed one critical fix for the COM_TABLE_DUMP vulnerability. This update properly fixes all of the issues.*** | **Debian:**<br>**http://security.debian.org/pool/updates/main/m/mysql/**<br>**MySQL:**<br>**http://www.mysql.com/downloads/mysql-3.23.html**<br>**Mandrake:**<br>**http://www.mandrakesecure.net/en/ftp.php**<br>**SuSE:**<br>**ftp://ftp.suse.com/pub/suse/**<br>**EnGarde:**<br>**ftp://ftp.engardelinux.org/pub/engarde/stable/updates**<br>**Conectiva:**<br>**ftp://atualizacoes.conectiva.com.br/**<br>**Trustix:**<br>**ftp://ftp.trustix.net/pub/Trustix/updates/**<br>***RedHat:***<br>***ftp://updates.redhat.com*** | **MySQL Multiple Vulnerabilities**<br>**CVE Names: CAN-2002-1373, CAN-2002-1374, CAN-2002-1375, CAN-2002-1376** | **Low/High**<br>**(High if arbitrary code can be executed)** | **Bug discussed in newsgroups and websites.**<br>**Vulnerability has appeared in the press and other public media.** |
| Noffle[104] | Unix | Noffle 1.0.1 | A memory corruption vulnerability exists, which could let a remote malicious user possible cause a Denial of Service or execute arbitrary code. | **Debian:**<br>http://security.debian.org/pool/updates/main/n/noffle/ | Noffle Remote Memory Corruption<br>CVE Name: CAN-2003-0037 | Low/**High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. |

[93] e-matters GmbH Security Advisory, December 12, 2002.
[94] EnGarde Secure Linux Security Advisory, ESA-20021213-033, December 13, 2002.
[95] OpenPKG Security Advisory, OpenPKG-SA-2002.013, December 16, 2002.
[96] Gentoo Linux Security Announcement, 200212-2.1, December 16, 2002.
[97] Debian Security Advisory, DSA-212-1, December 17, 2002.
[98] Conectiva Linux Security Announcement, CLA-2002:555, December 17, 2002.
[99] Mandrake Linux Security Update Advisory, MDKSA-2002:087, December 18, 2002.
[100] Trustix Secure Linux Security Advisory #2002-0086, TSLSA-2002-0086, December 19, 2002.
[101] SuSE Security Announcement, SuSE-SA:2003:003, January 2, 2003.
[102] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:288-22, January 15, 2003.
[103] EnGarde Secure Linux Security Advisory, ESA-20030127-001, January 27, 2003.
[104] Debian Security Advisory, DSA 244-1, January 27, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Nuke-browser[105] | Multiple | Nuke-browser 2.1, 2.3, 2.5, 2.11, 2.20, 2.41 | A vulnerability exists in 'nukebrowser.php' script file because it is possible to influence the include path, which could let a remote malicious user  include arbitrary files on the server. | No workaround or patch available at time of publishing. | Nukebrowser Remote File Include | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| NuKed-KlaN[106] | Multiple | NuKed-KlaN beta 1.2 | Cross-Site Scripting vulnerabilities exist in the Guestbook, Forum, and Shoutbox modules, which could let a remote malicious user execute arbitrary code. | Upgrade available at:<br>http://www.nuked-klan.org/ | NuKed-KlaN Remote Cross-Site Scripting | **High** | Bug discussed in newsgroups and websites. Exploits have been published. |
| **Open LDAP**[107]<br><br>***More upgrades issued***[108, 109, 110, 111,] | **Unix** | **OpenLDAP 2.0-2.0.23** | **Several buffer overflow vulnerabilities exist which could let a malicious user execute arbitrary code.** | **SuSE:**<br>**ftp://ftp.suse.com/pub/suse**<br><br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/ftp.php**<br>***RedHat:***<br>**ftp://updates.redhat.com/**<br>***Debian:***<br>**http://security.debian.org/pool/updates/main/o/openldap2/o**<br>***Conectiva:***<br>**ftp://atualizacoes.conectiva.com.br/6.0/RPMS** | **OpenLDAP Multiple Buffer Overflow**<br><br>**CVE Names: CAN-2002-1378, CAN-2002-1379** | **High** | **Bug discussed in newsgroups and websites.** |
| OpenBSD[112] | Unix | OpenBSD 2.6-22.9, 3.0-3.2 | A vulnerability exists in 'chpass' binary, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | OpenBSD CHPass Content Revealing | Medium | Bug discussed in newsgroups and websites. |
| Opera Software[113] | Windows | Opera Web Browser 7.0 win32 | A Cross-Domain Scripting vulnerability exists because it is possible for functions in different domains to be accessed and executed, functions can be executed under the caller's domain credentials, and it is possible to override properties and methods in other windows, which could let a malicious user execute arbitrary code. | Upgrade available at:<br>http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows | Opera Cross-Domain Scripting | **High** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.<br><br>Vulnerability has appeared in the press and other public media. |

[105] SecurityFocus, January 30, 2003.
[106] Security Corporation Security Advisory, SCSA-003, January 27, 2003.
[107] SuSE Security Announcement, SuSE-SA:2002:047, December 6, 2002.
[108] Conectiva Linux Security Announcement, CLA-2002:556, December 19, 2003.
[109] Debian Security Advisory, DSA 227-1, January 13, 2003.
[110] Mandrake Linux Security Update Advisory, MDKSA-2003:006, January 15, 2003.
[111] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:040-07, February 6, 2003.
[112] "After" Security Advisory, ASA-000, February 3, 2003.
[113] GreyMagic Security Advisory, GM#002-OP, February 4, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Opera Software[114] | Windows | Opera Web Browser 7.0 win32 | A information disclosure vulnerability exists due to the way some properties are exposed by the history object, which could let a malicious user obtain sensitive information. | Upgrade available at:<br>http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows | Opera Web History Object Information Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published.<br>Vulnerability has appeared in the press and other public media. |
| Opera Software[115] | Windows | Opera Web Browser 7.0 win32 | A vulnerability exists when generating HTML to display images or embedded media because the URL is incorrectly formatted or encoded to local files, which could let a malicious user obtain sensitive information. | Upgrade available at:<br>http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows | Opera Image Rendering HTML Injection | Medium | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.<br>Vulnerability has appeared in the press and other public media. |
| Opera Software[116] | Windows | Opera Web Browser 7.0 win32 | A vulnerability exists in the JavaScript console, which could let a malicious user execute arbitrary script. | Upgrade available at:<br>http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows | Opera JavaScript Console Attribute Injection | **High** | Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.<br>Vulnerability has appeared in the press and other public media. |
| Opera Software[117] | Windows | Opera Web Browser 7.0 win32 | A vulnerability exists due to a failure to ensure that a remote site has proper authorization, which could let a malicious user obtain sensitive information. | Upgrade available at:<br>http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows | Opera Error Message History Disclosure | Medium | Bug discussed in newsgroups and websites. Exploit has been published.<br>Vulnerability has appeared in the press and other public media. |

[114] GreyMagic Security Advisory, GM#005-OP, February 4, 2003.
[115] GreyMagic Security Advisory, GM#004-OP, February 4, 2003.
[116] GreyMagic Security Advisory, GM#003-OP, February 4, 2003.
[117] GreyMagic Security Advisory, GM#006-OP, February 4, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **PHP**[118]<br>***RedHat releases patch***[119] | **MacOS X 10.x, Unix** | **PHP 4.1.2, 4.2.0-4.2.3** | **A buffer overflow vulnerability exists in the wordwrap() function, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.** | **Upgrade available at:**<br>**http://www.php.net/downloads.php**<br>***RedHat:***<br>**ftp://updates.redhat.com/** | **PHP wordwrap() Buffer Overflow** | **Low/High**<br>**(High if arbitrary code can be executed)** | **Bug discussed in newsgroups and websites.** |
| phpLinks[120] | Multiple | phpLinks 2.x | A vulnerability exists in the 'email_confirmation.php' script, which could let a remote malicious user send arbitrary e-mail messages. | No workaround or patch available at time of publishing. | phpLinks Access Control | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| phpMy News Letter[121] | Unix | phpMy NewsLetter 0.6.10 | A vulnerability exists in the 'customize.php' script, which could let a malicious user execute arbitrary commands. | No workaround or patch available at time of publishing. | phpMyNews Letter Remote File Include | **High** | Bug discussed in newsgroups and websites. |
| **PHPOut-sourcing**[122]<br>***Upgrade now available***[123] | **Multiple** | **Zorum 3.0-3.2** | **A vulnerability exists due to the way PHP includes are handled, which could let a remote malicious user execute arbitrary commands.** | ***Upgrade available at:***<br>**http://zorum.phpoutsourcing.com/download.php** | **Zorum PHP Includes** | **High** | **Bug discussed in newsgroups and websites. Exploit has been published.** |
| plptools[124] | Unix | plptools 0.6 | A vulnerability exists in the 'plpnfsd' daemon because a logging function contains insecure syslog() calls, which could let a malicious user obtain elevated privileges. and execute arbitrary code. | Upgrade available at:<br>http://prdownloads.sourceforge.net/plptools/plptools-0.11.tar.gz?download | PLP Tools plpnfsd Syslog() Calls | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| qt-dcgui[125] | Unix | qt-dcgui 0.2, 0.2.1 | A vulnerability exists in the way directories are parsed, which could let a remote malicious user obtain sensitive information. | Upgrade available at:<br>http://dc.ketelhot.de/download.php | qt-dcgui Remote Directory Parsing F | Medium | Bug discussed in newsgroups and websites. |
| Qual-comm[126] | Multiple | Eudora 5.2 | A vulnerability exists due to the way e-mail messages are deleted from the 'Trash' folder, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Eudora E-mail Message Deletion | Medium | Bug discussed in newsgroups and websites. |

[118] Bugtraq, December 27, 2002.
[119] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:017-06, February 4, 2003.
[120] Bugtraq, January 20, 2003.
[121] Eclipse Advisory, February 5, 2003.
[122] Bugtraq, January 22, 2003.
[123] Bugtraq, January 26, 2003.
[124] Carl Livitt Security Vulnerability Advisory, CLIVITT-2003-2, January 29, 2003.
[125] Gentoo Linux Security Announcement, 200302-03, February 4, 2003.
[126] Bugtraq, January 24, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| RedHat[127] | Unix | Linux 6.2-i386, 7.0-i386, 7.1-i386, 7.2 - i386, ia64, 7.3-i386, 8.0-i386 | A vulnerability exists in the Kerberos ftp client when retrieving a file with a filename that begins with a pipe character, which could let a malicious user execute arbitrary commands. | Upgrade available at: ftp://updates.redhat.com/ | RedHat FTP Pipe<br>CVE Name: CAN-2003-0041 | **High** | Bug discussed in newsgroups and websites. |
| RedHat[128] | Unix | Linux 7.1, 7.2, 7.3, 8.0 | A vulnerability exists in the 'pam_xauth' module when running the 'su' utility in conjunction, which could let a malicious user obtain elevated privileges. | No workaround or patch available at time of publishing. | PAM pam_xauth Elevated Privileges<br>CVE Name: CAN-2002-1160 | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |
| Replicom[129] | Windows NT | ProxyView | A vulnerability exists because a default password is embedded for the Administrator account, which could let a remote malicious user obtain administrative access. | No workaround or patch available at time of publishing. | ProxyView Default Password | **High** | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Save-It Software Pty. Ltd.[130] | Multiple | Byte Catcher FTP 1.0.4 b | A buffer overflow vulnerability exists if a banner of excessive length is submitted, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. | No workaround or patch available at time of publishing. | ByteCatcher FTP Client Buffer Overflow | Low/**High**<br>**(High if arbitrary code is executed)** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Sebastian Bunka[131] | Unix | myphpPage tool 0.4.3-1 | A vulnerability exists in several of the PHP script files that are in the /doc/admin folder, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | myphpPage Tool Remote File Include | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Sharman Networks[132] | Windows | KaZaA Media Desktop 2.0 | A Denial of Service vulnerability exists due to a failure to sufficiently handle unsuspected responses to ad requests. Execution of arbitrary code may be possible. | No workaround or patch available at time of publishing. | KaZaA Advertisement Requests Denial of Service | Low/**High**<br>**(High if arbitrary code can be executed)** | Bug discussed in newsgroups and websites. Exploit has been published. |
| SILC[133] | Unix | Secure Internet Live Conferencing 0.9.11 | A vulnerability exists in error logging of the 'INVITE' command, which could let a malicious user cause a Denial of Service. | Upgrade available at: http://silcnet.org/index.php?page=download | SILC Server INVITE Command Denial of Service | Low | Bug discussed in newsgroups and websites. |

[127] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:242, January 31, 2003.
[128] Bedatec Security Advisory, 200212140001, February 4, 2003.
[129] Bugtraq, January 27, 2003.
[130] SecurityFocus, February 4, 2003.
[131] Bugtraq, February 2, 2003.
[132] Bugtraq, February 2, 2003.
[133] SecurityFocus, January 30, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| SILC[134] | Unix | Secure Internet Live Conferencing 0.9.11, 0.9.12 | A vulnerability exists because password authentication information is handled in an unsafe manner, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | SILC Server SSH2 Authentication Password | Medium | Bug discussed in newsgroups and websites. |
| Simon Tatham[135] | Windows 95/98/NT 4.0/2000 | PuTTY 0.48, 0.49, 0.53, 0.53b | A vulnerability exists because password authentication information is handled in an unsafe manner, which could let a malicious user obtain sensitive information. | No workaround or patch available at time of publishing. | Putty Authentication Password<br>CVE Name: CAN-2003-0048 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| slocate[136, 137] | Unix | slocate 2.6 | A buffer overflow vulnerability exists when the slocate program is run with command line arguments of excessive length, which could let a malicious user execute arbitrary code. | Upgrade available at: ftp://ftp.geekreview.com/slocate/src/slocate-2.7.tar.gz<br>**Mandrake:**<br>http://www.mandrakesecure.net/en/ftp.php | slocate Buffer Overrun | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Spam Assassin[138] | Unix | Spam Assassin 2.40-2.43 | A buffer overflow vulnerability exists when the e-mail system is using the 'spamc' program in BSMTP mode due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code. | Upgrade available at: http://spamassassin.org/released/Mail-SpamAssassin-2.44.tar.gz | SpamAssassin BSMTP Mode Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Spam Probe[139] | Unix | SpamProbe 0.8 a | A remote Denial of Service vulnerability exists when a specially crafted e-mail message is submitted. | Upgrade available at: http://prdownloads.sourceforge.net/spamprobe/spamprobe-0.8b.tar.gz?download | SpamProbe Remote Denial of Service | Low | Bug discussed in newsgroups and websites. |
| Sun Micro-systems, Inc.[140] | Unix | Solaris 2.5, 2.5.1, 2.6, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86 | Several vulnerabilities exist: a vulnerability exists in the 'at' utility due to improper sanitization of parameters, which could let a malicious user delete arbitrary files on the system; and a vulnerability exists when verifying the ownership of an 'at' job before deletion, which could let a malicious user delete arbitrary system files. | Patches available at: http://sunsolve.sun.com/pub-cgi/<br>Patch 108320-03,<br>Patch 108319-03,<br>Patch 109008-09,<br>Patch 108876-13,<br>Patch 109007-09,<br>Patch 108875-13,<br>Patch 114136-01,<br>Patch 114135-01 | Sun Solaris 'at' Command Race Condition | Medium | Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. |

[134] Bugtraq, February 1, 2003.
[135] iDEFENSE Security Advisory, January 28, 2003.
[136] USG Security Advisory, USG-SA-2003.001, January 24, 2003.
[137] Mandrake Linux Security Update Advisory, MDKSA-2003:015, February 5, 2003.
[138] Bugtraq, January 23, 2003.
[139] SecurityFocus, January 31, 2003.
[140] SecurityTracker Alert ID, 1005994, January 27, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Sun Micro-systems, Inc.[141] | Windows, Unix | Java Web Start 1.0, 1.0.1, 1.0.1_01, 1.0.1_02, 1.2;<br>JRE (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.3, 1.3_1.3, 1.3_02, 1.3_05, 1.3.1, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.1;<br>JSSE 1.0.3;<br>SDK (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.3_02, 1.3_05, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.0_02, 1.4, 1.4.1 | A vulnerability exists because the Java Secure Socket Extension (JSSE), Java Plug-in, and Java Web Start incorrectly validate the digital certificate of a web site, which could let untrustworthy web sites be authenticated for SSL transactions. | Upgrades available at:<br>http://java.sun.com/products/jsse/index-103.html<br>or<br>http://java.sun.com/j2se/ | Sun JSSE/Java Plug-In/Java Web Start Incorrect Certificate Validation | Medium | Bug discussed in newsgroups and websites. |
| Sun Micro-systems, Inc.[142] | Unix | Solaris 2.6, 7, 8, 9 | A remote Denial of Service vulnerability exists in the 'in.ftpd' daemon. | **Workaround:**<br>http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50240 | Solaris Remote Denial of Service | Low | Bug discussed in newsgroups and websites. |

[141] Sun(sm) Alert, 50081, January 23, 2003.
[142] Sun(sm) Alert, 50240, January 27, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Sun Micro-Systems, Inc.[143] | Windows, Unix | JRE (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.2.2, 1.2.2_010, 1.2.2_011, 1.2.2_13, 1.3, 1.3_02, 1.3_05, 1.3.1, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.0_02; SDK (Linux Production Release), (Solaris Production Release), (Windows Production Release) 1.2.2_010, 1.2.2_011, 1.2.2 _13, 1.3_02, 1.3_05, 1.3.1_01, 1.3.1_03, 1.3.1_05, 1.4, 1.4.0_02 | A vulnerability exists in the Java Virtual Machine that may allow illegal access to protected fields or methods of an object, which could possible let a malicious user execute arbitrary commands. | Upgrades available at: http://java.sun.com/j2se/ | Sun Java Virtual Machine Illegal Access To Object Methods | **High** | Bug discussed in newsgroups and websites. |
| SuSE[144] | Unix | Linux 8.1, Enterprise Server 8, Office Server, Open exchange Server 4 | A vulnerability exists in the 'susehelp' package due to inadequate filtering of user-supplied input to remove certain shell metacharacters, which could let a remote malicious user execute arbitrary commands. | Upgrade available at: ftp://ftp.suse.com/pub/suse/ | Linux 'susehelp' Input Validation | **High** | Bug discussed in newsgroups and websites. |

[143] Sun(sm) Alert Notification, 50083, January 23, 2003.
[144] SuSE Security Announcement, SuSE-SA:2003:005, January 20, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| Sygate[145] | Windows | Sygate Personal Firewall Pro 5.0 | A vulnerability exists because the default configuration of the firewall permits UDP packets to access open destination ports on the firewall-protected host if the packet source port is port 137 or 138, which could let a remote malicious user bypass the firewall. | Workaround available at:<br>http://archives.neohapsis.com/archives/ntbugtraq/2003-q1/0059.html | SyGate Firewall Bypass | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| Van Dyke Technologies[146] | Windows 95/98/NT 4.0/2000 | SecureCRT 3.4.7, 4.0.2; SecureFX 2.0.4, 2.1.2; ETunnel 1.0.2 | A vulnerability exists because password authentication information is handled in an unsafe manner, which could let a malicious user obtain sensitive information. | **SecureCRT:**<br>http://www.vandyke.com/download/securecrt/3.4/index.html<br>**SecureFX:**<br>http://www.vandyke.com/download/securefx/2.0/index.html<br>**ETunnel:**<br>http://www.vandyke.com/download/entunnel/index.html | SecureCRT, SecureFX, Entunnel Authentication Password<br>CVE Name: CAN-2003-0047 | Medium | Bug discussed in newsgroups and websites. There is no exploit code required. |
| **VIM Development Group[147]**<br>***Mandrake releases patch[148]*** | **Unix** | **VIM 5.0-5.8, 6.0, 6.1** | **A vulnerability exists in the modelines function due to insufficient handing of input, which could let a remote malicious user execute arbitrary code.**<br>***Note: A conceptual worm has been reported that explicitly illustrates how this vulnerability could be further exploited to act as a mass mailing worm.*** | **RedHat:**<br>**ftp://updates.redhat.com/**<br>***Mandrake:***<br>**http://www.mandrakesecure.net/en/ftp.php** | **VIM ModeLines Arbitrary Command Execution**<br>**CVE Name: CAN-2002-1377** | **High** | **Bug discussed in newsgroups and websites. VIM Worm has been published that exploits this vulnerability.** |
| **Web-cyradm[149]**<br>***Upgrade now available[150]*** | **Unix** | **Web-cyradm 0.5.1, 0.5.2** | **A remote Denial of Service vulnerability exists when the accompanying IMPA daemon is not running.** | ***Upgrade available at:***<br>http://www.web-cyradm.org/web-cyradm-cvs-2003-01-29.tar.gz | **Web-cyradm Remote Denial of Service** | **Low** | **Bug discussed in newsgroups and websites.** |

[145] NTBugtraq, January 22, 2003.
[146] iDEFENSE Security Advisory, January 28, 2003.
[147] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:297-17, January 16, 2003.
[148] Mandrake Linux Security Update Advisory, MDKSA-2003:012, February 3, 2003.
[149] DSINet Security Advisory, DSINET-SA-02-01, December 30, 2002.
[150] SecurityFocus, January 29, 2003.

| Vendor | Operating System | Software Name | Vulnerability/ Impact | Patches/Workarounds/ Alerts | Common Name | Risk* | Attacks/ Scripts |
|---|---|---|---|---|---|---|---|
| **Windowmaker[151]**<br>***RedHat issues upgrade*[152]** | **Unix** | **Windowmaker 0.20.1-3, 0.52-2, 0.53, 0.61, 0.61.1, 0.62, 0.62.1, 0.63, 0.63.1, 0.64, 0.65, 0.80** | **A buffer overflow vulnerability exists in the image handling code, which could let a remote malicious user execute arbitrary code.** | **Debian:**<br>**http://security.debian.org/pool/updates/main/w/wmaker/**<br>***RedHat:***<br>ftp://updates.redhat.com/6.2/en/os/ | **Window Maker Image Handling Buffer Overflow**<br>**CVE Name: CAN-2002-1277** | **High** | **Bug discussed in newsgroups and websites.** |
| YaBB SE[153] | Multiple | YaBB SE Forum 1.5.1 & prior | A vulnerability exists in the 'News.php' script, which could let a remote malicious user execute arbitrary code. | No workaround or patch available at time of publishing. | YaBB SE Forum 'News.php' Remote Code Execution | **High** | Bug discussed in newsgroups and websites. |
| ZyXel[154] | Multiple | Prestige 642, 642M, 642M-I, 642ME, 642R, 642R-I, 645 | A vulnerability exists in the administration interface because a pre-set default username and password exist, which could let a remote malicious user obtain sensitive information. | Until fixes/upgrades are available, contact your service provider for information on how to disable the default account. | DSL Modem Default Remote Administration Password | Medium | Bug discussed in newsgroups and websites. Exploit has been published.<br>Vulnerability has appeared in the press and other public media. |

*"Risk" is defined by CyberNotes in the following manner:

**High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

**Medium** – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

**Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[151] Debian Security Advisory, DSA-190-1, November 7, 2002.
[152] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:043-12, February 5, 2003.
[153] SecurityTracker Alert ID. 1005985, January 24, 2003.
[154] NTBugtraq, January 23, 2003.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between January 25 and February 5, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 14 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| **February 5, 2003** | **Icmp.c** | **Linux shellcode that creates a remote ICMP backdoor that can be controlled trough the ping utility.** |
| February 5, 2003 | Libexploitv01a.tar.gz | A generic exploit creation library to help write exploits to test a vulnerability. Using the API you can write buffer overflows (stack/heap/remote/local) and format strings fast and easily by taking care of a lot of the redundant code. |
| February 5, 2003 | Solaris-at.c | Script that exploits the Sun Solaris 'at' Command Race Condition vulnerability. |
| February 5, 2003 | SPIKE2.8.tgz | An easy to use generic protocol API that helps reverse engineer new and unknown network protocols. It features several working examples and includes a web server NTLM Authentication brute forcer and example code that parses web applications and DCE-RPC (MSRPC). |
| February 3, 2003 | Fstream-overflows.txt | This paper describes FILE stream overflow vulnerabilities and illustrates how they can be exploited. |
| February 3, 2003 | Prosrc.zip | An open source scanner that uses an ARP packet analyzing technique to detect network adapters that are in promiscuous mode. |
| **February 3, 2003** | **Xfiles.htm** | **Proof of Concept exploit for the Internet Explorer dragDrop Method vulnerability.** |
| **February 2, 2003** | **Blade586-942.wav** | **Exploit for the Bladeenc Signed Integer Memory Corruption vulnerability.** |
| February 2, 2003 | Ettercap-0.6.9.tar.gz | A network sniffer/interceptor/logger for switched LANs that uses ARP poisoning and the man-in-the-middle technique to sniff all the connections between two hosts. |
| January 31, 2003 | SP147.tgz | A web application analysis tool that uses the SPIKE API to help reverse engineer new and unknown network protocols. |
| January 30, 2003 | CLIVITT-2003-2.txt | Exploit for the PLP Tools plpnfsd Syslog() Calls vulnerability. |
| January 27, 2003 | Kismet-2.8.1.tar.gz | A 802.11b wireless network sniffer that is capable of sniffing using almost any wireless card supported in Linux, which currently divide into cards handled by libpcap and the Linux-Wireless extensions (such as Cisco Aironet), and cards supported by the Wlan-NG project which use the Prism/2 chipset (such as Linksys, Dlink, and Zoom). |
| January 27, 2003 | Mimedefang-2.29.tar.gz | A flexible MIME e-mail scanner designed to protect Windows clients from viruses and other harmful executables. |
| January 25, 2003 | Dhcp-expl.c | Exploit for the ISC dhcpd Format String vulnerability. |

## Trends

- **Systems are being compromised through the exploitation of null or weak default 'sa' passwords in Microsoft SQL Server and Microsoft Data Engine.**
- **Propagation of SQL 'Slammer' or 'Sapphire' malicious code is still causing varied levels of network degradation across the Internet and the compromise of vulnerable machines.**
- **NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm. For patch information, see:**
  - **http://www.microsoft.com/security/slammer.asp**
  - **http://www.microsoft.com/technet/security/bulletin/MS02-061.asp**
  - **http://www.microsoft.com/technet/security/bulletin/MS02-039.asp**
- **The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.**
- **The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.**
- **The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.**

## Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

| Ranking | Common Name | Type of Code | Trends | Date |
|---|---|---|---|---|
| 1 | W32/Klez | Worm | Stable | January 2002 |
| 2 | W32/Yaha | Worm | Increase | February 2002 |
| 3 | W32/Sobig | Worm | New to table | January 2003 |
| 4 | W32/Avril | Worm | New to table | January 2003 |
| 5 | W32/Bugbear | Worm | Decrease | September 2002 |
| 6 | JS/NoClose | Trojan | Increase | May 2002 |
| 7 | W32/SQLSlammer | Worm | New to table | January 2003 |
| 8 | Elkern | File Infector | Decrease | October 2001 |
| 9 | Funlove | File | Slight Increase | November 1999 |
| 10 | W32/Nimda | File, Worm | Return to table | September 2001 |

Note: Virus reporting may be weeks behind the first discovery of infection. A total 205 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 330 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

**JHC.1634 (DOS Virus):** This is a memory-resident DOS virus that infects the .exe, and .com files, as well as the Master Boot Record (MBR). The size of the infected files is increased by 1,634 bytes. The virus carries a destructive payload. If the virus is executed on June 17th, it attempts to overwrite with blank content any loaded and executed programs.

**JS/Fornightb@M:** This script virus resides on a website. When users visit this page, a link to this webpage is appended to their e-mail signature file for Outlook Express 5.0. When an infected user manually sends out an e-mail message, a link will appear at the bottom pointing to a web page on this site. The link to the infected webpage is included in an IFrame, so if the receiving e-mail client supported HTML, the page would open automatically and be displayed inside the e-mail message. The virus will create the file s.htm in the WINDOWS directory, which contains the IFrame link to the infected website address. It will then create an invalid Windows 'hosts' file. The Windows HOSTS file serves to associate host names with IP addresses. It is queried prior to any DNS queries being issued. The hosts file dropped by this virus contains of a list of URLs, each associated with a bogus IP address. The following registry keys will also be modified:

- HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Internet Explorer\\Control Panel\\SecurityTab,"1"
- HKEY_CURRENT_USER\\Software\\Policies\\Microsoft\\Internet Explorer\\Control Panel\\AdvancedTab,"1"

A patch for the vulnerability used is available from Microsoft at http://www.microsoft.com/technet/security/bulletin/MS00-075.asp.

**VBS_EVION.A (Aliases: VBS.Evion, VBS/Waterworks) (Visual Basic Script Worm):** This encrypted Visual Basic Script malware enumerates drives and overwrites files with the following extensions: VBS, HTM, HTML, ASP, HTX, and HTA. It also propagates through mIRC as the file JOKE.HTM. It carries the payload of displaying various message boxes depending on the system date. It runs on Windows 9x, ME, NT, 2K and XP systems.

**VBS_GAGGLE.C (Aliases: VBS/Gaggle@MM, VBS/Gaggle.B, I-Worm.Gaggl, VBS/Gaggle@mm*, VBS/Gaggl.Worm, VBS.Gaggle) (Visual Basic Script Worm):** This Visual Basic Script malware spreads via Internet Relay Chat using mIRC and by mass-mailing copies of itself to target e-mail addresses listed in the Microsoft Outlook address book. This worm overwrites .VBS files and infects all files with the following extensions in all folders and subfolders of local and mapped network drives: HTM, HTML, HTA, ASP, PHP, SHTM, SHTML, PHTM, and PHTML. This worm also deletes the following files upon execution:

- Regedit.exe
- Sfc.exe
- Msconfig.exe
- regedb32.exe

When the current system day is greater than 25, it changes the Internet Explorer home page. Also, whenever the sum of the current month and the current day is 30 (e.g. January 29 is 1 + 29 = 30), it displays a message box. This worm runs only on systems running Windows 95, 98, and ME.

**VBS_MOON.L (Visual Basic Script Worm):** This variant of VBS_MOON.A is a Visual Basic Script worm that modifies the homepage of Internet Explorer. The main propagation routine consists of sending itself via e-mail using Microsoft Outlook and via Internet Relay Chat using mIRC.

**VBS_SLUDGE.A (Aliases: VBS/Sludge.worm, Worm.P2P.Ikarus) (Visual Basic Script Worm):** This Visual Basic script worm uses KaZaA Lite in order to propagate. It creates copies of itself in the shared folder of KaZaA Lite using interesting file names, attracting other users into downloading it. On the system date, March 3, this VBScript worm displays a message box.

**W32.Bibrog@mm (Win32 Worm):** This is a mass-mailing worm that uses Microsoft Outlook to spread. When the worm is executed, it opens a program that looks like a shooting game. The e-mail message has the following characteristics:

- Subject: BigBrother Mexico Shooter
- Message: BigBrother Mexico Shooter Atinale a todos
- Attachment: Bigburros.exe

W32.Bibrog@mm is written in Microsoft Visual Basic 5 and is compressed with UPX.

**W32.Felic (Win32 Virus):** This is a virus that copies itself to the hard drive and floppy disk drive. The virus file uses a standard Windows folder icon to make you believe that it is a real folder. As a result, when you double-click the folder icon, the virus executes. If the system date is May 1st, September 9th, or December 2nd, and the system time is 00:00:00, W32.Felic displays an image and a message. This threat is written in the Microsoft Visual Basic programming language.

**W32.HLLW.Gemel (Alias: W32/Gemel.worm, W32/P2P.Torres.Worm, Worm.P2P.Gemel.a, WORM_GEMEL.A) (Win32 Worm):** This is a worm that attempts to spread through the Grokster, Morpheus, and KaZaA file-sharing networks. This worm also spreads through ICQ and floppy disks. This threat has several versions, and all the versions are written in the Microsoft Visual Basic programming language. It may be compressed with UPX or tElock.

**W32/Opaserv-L (Aliases: Worm.Win32.Opasoft.G, W32/Opaserv.worm.gen) (Win32 Worm):** This is a member of the W32/Opaserv family. When run, it copies itself into the Windows folder as svr32.exe and sets the following registry entry to run itself automatically when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Svr32 = C:\Windows\svr32.exe

W32/Opaserv-L spreads over the Internet using Windows network shares. The worm copies itself over to the Windows folder of the remote computer as svr32.exe and sets the following entry in the [Windows] section of win.ini, “run=C:\Windows\svr32.exe.” This entry will start the worm on the remote computer when Windows starts up. W32/Opaserv-L will attempt to remove older variants of the W32/Opaserv worm by removing the following files from the Windows folder:

- alevir.exe
- scrsvr.exe
- brasil.exe

The following registry entries will also be removed:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SCRSVR
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ALEVIR
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\BRASIL

**W97M.Blackout.Worm (Word 97 Macro Virus):** This is a Microsoft Word 97 macro worm that attempts to spread using mIRC. The file name that it uses is Readme.txt.doc.

**W97M.HashiBirth (Alias: Word97Macro/Opey.BF) (Word 97 Macro Virus):** This is a Word 97 macro virus that infects Microsoft Word documents and templates, as well as changes the appearance of Microsoft Word documents. This virus displays date-specific messages and animated text in Word documents. Once an infected document is opened, closed, and saved, the macro virus replicates itself to the document and to the Microsoft Word template file, Normal.dot.

**Worm/Bun.gen (Alias: IRC-Worm.Generic) (Internet Worm):** This is an Internet worm that spreads through e-mail by using addresses it collects in the Windows Address Book, through the use of the mIRC network, as well as, through the file-sharing program KaZaA. The worm arrives through e-mail in the following format:

- Subject: sex for FREE
- Body: Hi!hope you like this...you'll get 600+ sex pictures..for free..just run this attachment..
- Attachment: sexXX09.EXE.bat

If executed, the file DONKEY.VBS (614 bytes) will get dropped by the worm containing the send routine in order to replicate via Microsoft Outlook. After it send itself over Outlook to all e-mail contacts in the WAB (Windows Address Book), via the IRC program 'mIRC' and the P2P network program KaZaA. The worm will then override the autoexec.bat. The following registry keys also get created:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent "DisableSharing"=dword:00000000 "DownloadDir"="C:\\Program Files\\KaZaA\\My Shared Folder" "Dir0"="012345:c:\\"

**Worm/Hotcakes.gen (Alias: IRC-Worm.Generic) (Internet Worm):** This is an Internet worm that spreads through e-mail by using addresses it collects in the Windows Address Book, as well as, through the use of the mIRC network. The worm arrives through e-mail in the following format:

- Subject: Patch your system now!!
- Body: Here's a patch that is newly discovered
- Attachment: hotcakes.bat

If executed, the file X.VBS (556 bytes) will get dropped by the worm containing the send routine in order to replicate via Microsoft Outlook. After it send itself over Outlook to all e-mail contacts in the WAB (Windows Address Book) and via the IRC program 'mIRC'. There are no new registry key entries.

**WORM_LOLOL.B (Aliases: Worm/Lolol, W32/Lolol-B, Win32/HLLW.Lolol.B, Worm.P2P.Lolol.b, W32/Lolol.worm.gen) (Internet Worm):** This variant of WORM_LOLOL.A propagates via shared folders of the KaZaA peer-to-peer file sharing application. When memory-resident, it connects to a specific Internet Relay Chat (IRC) server where it receives commands from a remote user to process locally on the affected system. This malware works on Windows 95, 98, NT, 2000, ME, and XP systems.

**WORM_LOLOL.C (Aliases: Worm.P2P.Lolol.c, Win32/HLLW.Lolol.C, W32/Lolol-C) (Internet Worm):** This memory-resident worm propagates via the file-sharing network of KaZaA. It is a variant of WORM_LOLOL.A and similarly has backdoor capabilities. Once active on the target system, it connects to a specific Internet Relay Chat (IRC) server where it receives commands from a remote user to process locally on the affected system. Its behavior is entirely similar to the A variant except for one of its dropped files, its process name and its created autostart registry entries. This worm program runs on Windows 95, 98, NT, 2000, ME and XP systems.

**WORM_LOLOL.D (Aliases: Worm.P2P.Lolol.d, Win32/HLLW.Lolol.D, W32/Lolol-D) (Internet Worm):** This variant of WORM_LOLOL.A has both worm and backdoor capabilities. As a worm, it propagates via the popular file-sharing network of KaZaA. Once active on its target system, it connects to a specific Internet Relay Chat (IRC) server, where it receives commands from a remote user and processes it locally on the affected system. Its behavior is highly similar to WORM_LOLOL.A. It differs only in its additional backdoor capabilities. This malicious program runs on Windows 95, 98, NT, 2000, ME and XP systems.

**WORM_LOLOL.E (Aliases: W32/Lolol-E, Win32/HLLW.Lolol.E, W32/Lolol.worm.gen, Worm/Lolol, Worm.P2P.Lolol.e) (Internet Worm):** This variant of WORM_LOLOL.A propagates by dropping multiple copies of itself into the shared folders of the KaZaA peer-to-peer file sharing application. When memory-resident, it connects to certain Internet Relay Chat (IRC) servers, where it receives commands from a remote user to process locally on the affected system. This malware, after connecting to IRC, allows remote malicious users to do the following on affected machines:

- retrieve system information such as CPU speed, operating system (current Windows version build), RAM size, IP address, host name, and Internet connection type
- open a specified URL remotely
- use the affected system to PING and send packets to other hosts
- create clones on a specified channels
- execute a file remotely
- command the backdoor worm to download an updated copy itself

This malware runs on Windows 95, 98, ME, NT, 2000, and XP.

**WORM_OPASERV.Q (Aliases: W32/Opaserv-J, W32/Opaserv.worm, Worm.Win32.Opasoft.f, I-Worm/Opas.Q, W32/Opaserv.worm.N) (Internet Worm):** This worm propagates via network shared C:\ drives and downloads an executable file, from a specific Web site. It modifies the registry of its infected systems so that is automatically executes during Windows startup. This worm runs on all Windows platforms.

**WORM_OPASERV.R (Aliases: W32/Opaserv.worm.r, W32/Opaserv.worm.O, Trojan.Win32.OpaKill.c, Win32/Opaserv.M.worm, W32/Opaserv-K, Win32.Opaserv.R) (Internet Worm):** This destructive, memory-resident worm is a slightly modified version of WORM_OPASERV.H. Like earlier OPASERV variants, it propagates via shared network drives. When the system date is anywhere between December 24 to 31 or the year is greater than 2002, this worm carries out its destructive routines. The following are some of its most destructive routines:

- overwrite the boot sector of the infected system
- destroy the CMOS
- delete files from the hard drive

These routines practically leave the infected system unusable. It also modifies the registry and the configuration file, WIN.INI, so that it automatically executes every Windows startup. It utilizes a known exploit that enables malicious users to access shared drives, as discussed in a security patch from Microsoft. This worm runs on all Windows platforms.

**WORM_SYTRO.A (Aliases: W32/Sytro.worm.a, Worm.P2P.Sytro.a, Win32.HLLW.Electron.A worm) (Internet Worm):** This nondestructive, UPX-compressed worm spreads via the KaZaA file-sharing network. To propagate via KaZaA, it creates a folder named "SysConfig" in the Windows directory, and then drops several copies of itself in the said folder. It then adds an entry in the registry to enable the sharing of the created folder over the KaZaA file-sharing network. This worm is developed in Delphi and runs on Windows 95, 98, ME, NT, 2000, and XP.

**WORM_WINUR.A (Alias: W32.HLLW.WINUR) (Internet Worm):** This peer-to-peer (P2P) worm spreads through the KaZaA and the WinMX file sharing networks. It also spreads to shared network drives with write access and drops a copy of itself on loaded floppy disks. It configures MSN messenger to prompt users into sending a copy of itself to other MSN users. This worm also has the capability to perform Denial of Service (DoS) attacks against certain web sites. It runs on Windows 95, 98, ME, 2000, and XP.

## *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Backdoor.Amitis | N/A | CyberNotes-2003-01 |
| Backdoor.Assasin.D | D | CyberNotes-2003-01 |
| Backdoor.Beasty | N/A | CyberNotes-2003-02 |
| **Backdoor.Beasty.B** | **B** | **Current Issue** |
| **Backdoor.CHCP** | **N/A** | **Current Issue** |
| Backdoor.Colfuser | N/A | CyberNotes-2003-01 |
| Backdoor.Cow | N/A | CyberNotes-2003-01 |
| Backdoor.Cybspy | N/A | CyberNotes-2003-01 |
| Backdoor.Deftcode | N/A | CyberNotes-2003-01 |
| Backdoor.Drator | N/A | CyberNotes-2003-01 |
| Backdoor.FTP.Casus | N/A | CyberNotes-2003-02 |
| Backdoor.Hethat | N/A | CyberNotes-2003-01 |
| Backdoor.Hornet | N/A | CyberNotes-2003-01 |
| Backdoor.IRC.Aladinz | N/A | CyberNotes-2003-02 |
| **Backdoor.Krei** | **N/A** | **Current Issue** |
| Backdoor.Lala | N/A | CyberNotes-2003-01 |
| Backdoor.Massaker | N/A | CyberNotes-2003-02 |
| Backdoor.NetDevil.B | B | CyberNotes-2003-01 |
| Backdoor.NetTrojan | N/A | CyberNotes-2003-01 |
| Backdoor.Ohpass | N/A | CyberNotes-2003-01 |
| Backdoor.OICQSer.165 | N/A | CyberNotes-2003-01 |
| Backdoor.OICQSer.17 | 17 | CyberNotes-2003-01 |
| Backdoor.OptixPro.10.c | 10.c | CyberNotes-2003-01 |
| Backdoor.Remohak.16 | 16 | CyberNotes-2003-01 |
| Backdoor.RemoteSOB | N/A | CyberNotes-2003-01 |
| Backdoor.Rephlex | N/A | CyberNotes-2003-01 |
| Backdoor.Sdbot.C | C | CyberNotes-2003-02 |
| **Backdoor.Sdbot.D** | **D** | **Current Issue** |
| **Backdoor.Serpa** | **N/A** | **Current Issue** |
| Backdoor.Servsax | N/A | CyberNotes-2003-01 |
| Backdoor.Sixca | N/A | CyberNotes-2003-01 |
| Backdoor.Talex | N/A | CyberNotes-2003-02 |
| **Backdoor.Udps.10** | **10** | **Current Issue** |
| Backdoor.Upfudoor | N/A | CyberNotes-2003-01 |
| Backdoor.VagrNocker | N/A | CyberNotes-2003-01 |
| Backdoor.Vmz | N/A | CyberNotes-2003-01 |
| Backdoor.Xenozbot | N/A | CyberNotes-2003-01 |
| **Backdoor.Xeory** | **N/A** | **Current Issue** |
| Backdoor.Zdemon | N/A | CyberNotes-2003-02 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| Backdoor.Zix | N/A | CyberNotes-2003-02 |
| **Backdoor.Zvrop** | **N/A** | **Current Issue** |
| Backdoor-AOK | N/A | CyberNotes-2003-01 |
| BDS/AntiPC | N/A | CyberNotes-2003-02 |
| BDS/Backstab | N/A | CyberNotes-2003-02 |
| **BDS/Evolut** | **N/A** | **Current Issue** |
| Downloader-BO.dr.b | N/A | CyberNotes-2003-02 |
| Downloader-BS | N/A | CyberNotes-2003-02 |
| **Exploit-IISInjector** | **N/A** | **Current Issue** |
| IRC/Backdoor.e | E | CyberNotes-2003-01 |
| IRC/Backdoor.f | f | CyberNotes-2003-02 |
| **IRC/Backdoor.g** | **g** | **Current Issue** |
| **IRC/Flood.bi** | **N/A** | **Current Issue** |
| **IRC-Emoz** | **N/A** | **Current Issue** |
| IRC-OhShootBot | N/A | CyberNotes-2003-01 |
| JS.Seeker.J | J | CyberNotes-2003-01 |
| **Keylog-Razytimer** | **N/A** | **Current Issue** |
| KeyLog-TweakPan | N/A | CyberNotes-2003-02 |
| MultiDropper-FD | N/A | CyberNotes-2003-01 |
| **ProcKill-Z** | **N/A** | **Current Issue** |
| PWSteal.AlLight | N/A | CyberNotes-2003-01 |
| PWSteal.Rimd | N/A | CyberNotes-2003-01 |
| **PWSteal.Senhas** | **N/A** | **Current Issue** |
| PWS-Tenbot | N/A | CyberNotes-2003-01 |
| QDel359 | N/A | CyberNotes-2003-01 |
| **Renamer.c** | **N/A** | **Current Issue** |
| TR/Fake.YaHoMe.1 | N/A | CyberNotes-2003-02 |
| TR/WinMx | N/A | CyberNotes-2003-02 |
| Troj/Dloader-BO | N/A | CyberNotes-2003-02 |
| **Troj/Manifest-A** | **N/A** | **Current Issue** |
| Troj/Qzap-248 | N/A | CyberNotes-2003-01 |
| **Troj/SadHound-A** | **N/A** | **Current Issue** |
| **Troj/Slanret-A** | **N/A** | **Current Issue** |
| TROJ_JBELLZ.A | A | CyberNotes-2003-02 |
| TROJ_KILLBOOT.B | B | CyberNotes-2003-01 |
| Trojan.Dasmin | N/A | CyberNotes-2003-01 |
| **Trojan.Dasmin.B** | **B** | **Current Issue** |
| Trojan.Downloader.Inor | N/A | CyberNotes-2003-02 |
| Trojan.Ivanet | N/A | CyberNotes-2003-02 |
| Trojan.KKiller | N/A | CyberNotes-2003-01 |
| Trojan.Poldo.B | B | CyberNotes-2003-02 |
| Trojan.PSW.Platan.5.A | N/A | CyberNotes-2003-01 |
| Trojan.PWS.QQPass.D | N/A | CyberNotes-2003-02 |
| Trojan.Qforager | N/A | CyberNotes-2003-02 |
| Trojan.Qforager.Dr | N/A | CyberNotes-2003-02 |
| Trojan.Qwe | N/A | CyberNotes-2003-02 |
| Trojan.Snag | N/A | CyberNotes-2003-02 |
| Trojan.Unblockee | N/A | CyberNotes-2003-01 |
| VBS.Moon.B | B | CyberNotes-2003-02 |

| Trojan | Version | CyberNotes Issue # |
|---|---|---|
| VBS.StartPage | N/A | CyberNotes-2003-02 |
| W32.Socay.Worm | N/A | CyberNotes-2003-02 |
| **W32.Systentry.Trojan** | **N/A** | **Current Issue** |
| W32.Xilon.Trojan | N/A | CyberNotes-2003-01 |
| **Xin** | **N/A** | **Current Issue** |

**Backdoor.Beasty.B (Alias: Trojan Beast 1.91):** This is a backdoor Trojan, which is similar to Backdoor.Beasty. It gives a malicious user complete access to the infected computer. By default, the Trojan listens on port 666 and notifies the malicious user through e-mail or ICQ. The Trojan attempts to terminate various security products and system monitoring tools. Backdoor.Beasty.B Trojan was created using Delphi.

**Backdoor.CHCP:** This is a backdoor Trojan that is written in the Microsoft Visual Basic programming language. The Trojan uses the same icon used by the Windows Notepad program in an attempt to deceive you into believing that it is a real Notepad text editor. Allows a malicious user to remotely control an infected computer. The Trojan opens TCP port 1145 by default.

**Backdoor.Krei:** This is a backdoor Trojan that uses Trojan.Slanret to hide its malicious activities. It opens a listening port (port 449 by default) on the infected computer and it gives a malicious user full access to the infected system.

**Backdoor.Sdbot.D:** This is a variant of Backdoor.Sdbot. It attempts to create these files:

- %Windir%\System32\Directx.exe
- %Windir%\System32\Sqlexploit.exe
- %Windir%\System32\NTCmd.exe
- %Windir%\System32\PipeCmd.exe
- C:\Directx.exe
- C:\Sqlexploit.exe

This Trojan adds the value, “directx  <path.to.the.trojan>,” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

This allows the malicious user to perform these additional actions:

- Perform an SQL scan.
- Start an FTP server on the infected computer.
- Dial any number using the modem.

**Backdoor.Serpa:** This is backdoor Trojan that opens a listening port (port 1,871 by default) on the infected computer. This gives a malicious user full access to the infected system. It can steal the CD Keys for several popular games and send them to a specified ICQ address.

**Backdoor.Udps.10 (Aliases: Backdoor.Udps.10.b, TROJ_UDPS10.A):** This is a backdoor Trojan that gives a remote malicious user full access to your computer. By default it listens for incoming connections on ports 101 and 1700. The existence of the files udps.exe or isatray.exe may indicate a possible infection.

**Backdoor.Xeory:** This is backdoor Trojan that, by default, opens ports 80 and 81 on an infected computer. The malicious user can steal your RAS passwords and system information and log your keystrokes.

**Backdoor.Zvrop:** This is a backdoor Trojan that allows unauthorized access to the infected computer. It copies itself to the %System% folder as these files:

- RegeditExec.exe
- WinLogin.exe

The default ports on which the server listens are 4,527, 3,527, and 2,527.

**BDS/Evolut:** Like other backdoors, BDS/Evolut would potentially allow someone with malicious intent remote access to your computer. If executed, the Trojan adds the following file to the \windows\%system% directory:

- index.html
- EVO_2003-02-06_7-41.html
- syspass.html

It will also copy itself to "C:\windows\system\netbi0s.exe." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Netbi0s"="C:\\WINDOWS\\system\\netbi0s.exe"

**Exploit-IISInjector:** This Trojan exploits an old IIS buffer overflow vulnerability that allows for the execution of arbitrary code on an unprotected IIS4 web server. For more information on this vulnerability see Microsoft Security Bulletin (MS99-019) located at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms99-019.asp.

**IRC/Backdoor.g:** This Trojan consists of an RC script files and a batch file. It is being distributed in a self-extracting archive, along with several other Trojans and attack tools. The mIRC scripts are designed to allow a remote IRC user to send commands the these various Trojans. One package received contained the following components.

- BackDoor-GI
- DDoS-Smurf
- Exploit-IISInjector
- FDoS-Wping
- FDoS-SynKal
- HideWindow application
- RemoteProcessLaunch application

The two script files use the various Trojans and applications to attack a remote system and conceal its presence on the host system.

**IRC-Emoz:** When this Trojan is run, it copies itself to "%windir%\system\.exe," where %windir% is the directory Windows is installed in. It adds the following registry key so that it launches itself everytime after a restart:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Network Socket Update

with the value: netsock.drv. Other Registry keys that are created are:

- HKEY_CLASSES_ROOT\NMCHANXCON
- HKEY_CLASSES_ROOT\NMCHANXCON\Join
- HKEY_CLASSES_ROOT\NMUSRXCON

It connects to an IRC channel and accepts commands from there.

**IRC/Flood.bi:** This is an IRC Trojan inside of a script that is used by mIRC - an 'Internet Chat Relay' client. Machines with mIRC clients running this script, can be remotely controlled and misused by a malicious user. Infected machines should be carefully examined, since it is possible that the malicious user has installed further Backdoors. It does not add, remove or change any Registry keys, although it's possible that keys have been altered by an attacker.

**Keylog-Razytimer:** When the Trojan runs, the file copies itself to the %windows\%system directory and makes a registry entry to load itself automatically at system start. For example on a Windows9X/ME based system:

- HKLM\Software\Mirosoft\Windows\CurrentVersion\Run\ "c:\windows\system\mshtml.exe"

To make the file less suspicious, the chosen name (mshtml.exe) is very close to regular system files like mshtml.dll. The Trojan is a called keylogger and attempts to retrieve user credentials like logon names and password. This information is gathered and together with a .jpg screenshot of the victim's user system can be transferred to a website. If the Serverlogger accepts the connection and the transfer is completed, it disconnects the client connection. The serverport in use is: 11831 The transferport is: 29559.

**ProcKill-Z:** This Trojan attempts to terminate the process of the numerous security programs. It does not add itself to any autostart keys or copy itself to the Windows directory, so simply rebooting the computer will clear the Trojan from memory. However, a dropper or installer component could install it to run at Windows startup.

**PWSteal.Senhas:** This is a UPX-packed, password stealing Trojan that attempts to disguise itself as Macromedia's Flash Player. It is written in the Borland Delphi programming language. Because this threat has  been modified, UPX cannot unpack it.

**Renamer.c:** This Trojan renames several system files, so that the system won't be able to boot the next time. It does not change, add or delete any Registry keys.

**Troj/Manifest-A (Aliases: ManifestDest trojan, W32.Manifest.Trojan):** This is a backdoor Trojan that allows unauthorized access of a computer from a remote location. It pretends to be an installation program for XviD MPEG-4 Codec. Upon execution, the Trojan installs the above program but then drops the various files to the folder C:\<Program Files>\Common Files\Services. It makes use of some legitimate software to allow unauthorized access and to monitor the victim computer, e.g. it makes use of an FTP server pogrom along with an altered initialization file Serv-u.ini which allows a remote intruder to upload or download files.  Troj/Manifest-A sets the following registry entries so that the Trojan and the legitimate software it uses are run on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Enumerate Service = "C:\Program Files\Common Files\Services\wsys.exe"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Folder Service = "C:\<Program Files>\Common Files\Services\wssdtu.exe"
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Serv-U = "C:\Program Files\Common Files\Services\wssdsu.exe"

**Troj/SadHound-A (Aliases: TrojanDropper.Win32.Small.aa, Backdoor.Welkom, TROJ_SADHOUND.A, Backdoor.Sadhound, Multidropper-CE, Sadhound):** This Trojan has two components, a dropper and an IRC backdoor Trojan. The dropper creates the IRC backdoor Trojan and a text file in the Windows temp folder. The backdoor Trojan is executed by the dropper, causing it to be copied to the Windows system folder with the filename MSWINS0CK.EXE, and creates the following registry entry so that the backdoor is executed when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft auto update = MSWINS0CK.EXE

The IRC backdoor Trojan connects to an IRC server and joins a specific channel. The server then waits for an attacker to join this channel and issue commands to run on the victim's computer.

**Troj/Slanret-A (Aliases: Backdoor.Ierk, Backdoor-ALI.sys):** This is a Trojan that may be used as a driver component, with the filename ierk8243.sys, by another application to gain unauthorized shared stealth access to the target computer.  Upon execution, the malicious application would install Troj/Slanret-A as a device with the name Mp437bba8e and may set the following registry entry:

- HKLM\System\CurrentControlSet\Services\Ierk8243

Functioning as a device, Troj/Slanret-A provides an interface that allows an application to run hidden with full system privileges.

**Trojan.Dasmin.B:** This is a Trojan horse and a variant of Trojan.Dasmin. It tries to disguise the files it creates as Windows System files. Trojan.Dasmin.B also sends users to specific Web pages, so that a counter on a page is incremented with each page hit. The author of this Trojan horse probably set up the Web page. This threat is compressed with UPX.

**W32.Systentry.Trojan (Alias: TROJ_SYSTENTRY.A):** This Trojan contacts a remote Web site from which it downloads a file. Then, it executes the downloaded file onto your computer. W32.Systentry.Trojan also locates the user information on your computer and sends it to a predetermined list of e-mail addresses. The list of addresses is downloaded from the same Web site as the downloaded file.

**Xin:** This Trojan is designed to play nasty tricks once installed on the victim PC. When it is executed, the Trojan copies itself to the %WinDir%\System directory (with a random filename), hooking system startup by adding a Registry key. For example:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "(Default)" = c:\WINDOWS\SYSTEM\EECCGAG.EXE

The following Registry key is also added:

- HKEY_LOCAL_MACHINE\Software\TheNix

Once installed on the victim machine, the Trojan periodically disrupts the mouse and keyboard, and spawns processes in order to consume system memory.